DETAILED ACTION

1. This is in reply to **REQUEST FOR CONTINUED EXAMINATION (RCE)** filed on 11/10/2008. **Claims 1-13** are cancelled; and **Claims 14-25** are new.

2. **Claims 14-25** are pending.

Priority

3. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 10/788,523, filed on 02/27/2004.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

5. Authorization for this examiner's amendment was given in a telephone interview with **Brad Spencer** [Reg. No. 57,076] on 12/16/2008.

The application has been amended as follows: In the claims,

14. (**Currently Amended**): An application authentication system comprising:

a terminal device on which an application is operated; and

a secure device connected fixedly or detachably to the terminal device,

wherein the terminal device includes:

a memory comprising an application recording unit configured to record the application which is operated on the terminal device and performs processing using data held by the secure device; and application running unit configured to run the application,

wherein the secure device includes:

another memory comprising a data holding unit configured to hold the data used by the application which is operated on the terminal device;

verifying unit configured to verify validity of the application running **unit** ~~means~~ and validity of the application; and

accepting unit configured to accept access from the application to the data held in the data holding **unit** ~~means~~ when the validities of the application running **unit** ~~means~~ and the application are authenticated,

wherein the application running **unit** ~~means~~ calculates digest data of the application and sends the digest data to the verifying **unit** ~~means~~ after the validity of the application running **unit** ~~means~~ is authenticated by the verifying **unit** ~~means~~, and

wherein the verifying **unit** ~~means~~ verifies the validity of the application using the transmitted digest data.

15. (**Currently Amended**): A secure device connected fixedly or detachably to a terminal which includes application running unit configured to run an application, the secure device comprising:

a memory comprising a data holding unit configured to hold data used by the application;

verifying unit configured to verify validity of the application running **unit** ~~means~~ and validity of the application; and accepting unit configured to accept access from the application to the data held in the data holding **unit** ~~means~~ when the validities of the application running **unit** ~~means~~ and the application are authenticated,

wherein the application running **unit** ~~means~~ of the terminal calculates digest data of the application and sends the digest data to the verifying **unit** ~~means~~ after the validity of the application running **unit** ~~means~~ is authenticated by the verifying **unit** ~~means~~, and

wherein the verifying **unit** ~~means~~ verifies the validity of the application using the transmitted digest data.

16. (**Currently Amended**): The secure device according to claim 15, wherein

an electronic signature is attached to the application by a certificate authority,

the application running **unit** ~~means~~ transmits the electronic signature attached to the application to the secure device,

the verifying **unit** ~~means~~ verifies the electronic signature by using a pubic key of the certificate authority and the digest data, and authenticates the application when a result of the verification is normal.

17. (**Currently Amended**): The secure device according to claim 15, wherein the verifying **unit** ~~means~~ holds the digest data of the application in advance, collates the held digest data and the transmitted digest data, and authenticates the application when the result of the collation is normal.

18. (**Currently Amended**): A terminal connected fixedly or detachably to a secure device which holds data used by an application operated on the terminal, verifies validity of running unit configured to run the application, verifies validity of the application using digest data of the application calculated by the running **unit** ~~means~~, validity of which is authenticated, accepts access by the application to the data when the validities of the running **unit** ~~means~~ and the application are authenticated, the terminal comprising:

the running unit configured to run the application;

a memory comprising an application recording unit configured to record the application which is operated on the terminal and performs processing using the data held by the secure device; and

recording unit configured to record the running **unit** ~~means~~ which runs the application,

wherein the running **unit** ~~means~~ calculates the digest data of the application and sends the digest data to the secure device when the running **unit** ~~means~~ is authenticated by the secure device.

19. (**Currently Amended**): The terminal according to claim 18, wherein the running **unit** ~~means~~ calculates the digest data after the application requests to use the data held by the secure device.

20. (**Currently Amended**): The terminal according to claim 18, wherein the running **unit** ~~means~~ is recorded in an unwritable area in the terminal, in which information are never rewritten by the operation on the terminal device, and the access from an external device.

21. (**Currently Amended**): An authenticating method used in a secure device ~~which~~**, comprising a memory, and that** is fixedly or detachably connected to a terminal which includes running unit configured to running an application, the method comprising:

providing, in the secure device, data holding unit configured to hold data used by the application which is operated on the terminal, verifying unit configured to perform authentication, and accepting unit configured to accept access to the data;

verifying validity of the running **unit** ~~means~~ by the verifying **unit** ~~means~~;

calculating digest data of the application and transmitting the digest data to the verifying **unit** ~~means~~ if the validity of the running **unit** ~~means~~ is authenticated by the verifying **unit** ~~means~~;

verifying validity of the application on the terminal by the verifying **unit** ~~means~~ using the transmitted digest data; and

accepting, by the accepting **unit** ~~means~~, access from the application to the data held by the data holding **unit** ~~means~~ when the validities of the running **unit** ~~means~~ and the application are authenticated.

22. (**Currently Amended**): An application authentication system comprising:

a secure device for managing data used by an application**, the secure device comprising a memory**; and

running unit configured to run a Basic Input Output System (BIOS), an Operating System (OS) operated on the BIOS, executing software operated on the OS and executing the application, and the application, wherein the secure device verifies validity of the BIOS,

wherein the BIOS verifies validity of the OS after the verification by the secure device,

wherein the OS verifies validity of the executing software after the verification by the BIOS,

wherein the executing software performs at least a part of processing of verifying validity of the application after the verification by the OS, and

wherein the secure device allows the application to use the data after the validity of the application is verified.

23. (Previously Presented): The application authentication system according to claim 22, wherein

the application transmits a command to the secure device after the validity of the application is verified by the executing software, and

the secure device accepts the command only when the verification of the validity of the application is successful.

24. (Previously Presented): The application authentication system according to claim 22, wherein

the executing software transmits information including a Hash of the application to the secure device, and

the secure device verifies validity of the information including the Hash of the application.

25. (**Currently Amended**): A method used in a system having a secure device for managing data used by an application **and comprising a memory**, and running unit configured to run a Basic Input Output System (BIOS), an Operating System (OS) operated on the BIOS, executing software operated on the OS and executing the application, and the application, the method comprising:

verifying validity of the BIOS by the secure device;

verifying validity of the OS by the BIOS after the verification by the secure device;

verifying validity of the executing software by the OS after the verification by the BIOS;

performing at least a part of processing of verifying validity of the application by the executing software after the verification by the OS; and

allowing the application to use the data by the secure device after the validity of the application is verified.

Allowable Subject Matter

Note: In view of further reading and updated search, examiner and applicants' representative agreed to make the examiner's amendment shown above. By this amendment **Claims 14-22 and 25** are amended.

6. **Claims 14-25** are allowed in view of amendments and arguments filed on 11/10/2008.

CONTACT INFORMATION

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2439)

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434